Get centralized EventLogs

…from all your computers in a single and clear place

Agenda

- Basics about Windows Event Forwarding platform
- How to operate with EventLogSubscriptions
- Q&A

Get-Person -Short

Andreas Bellstedt

@AndiBellstedt

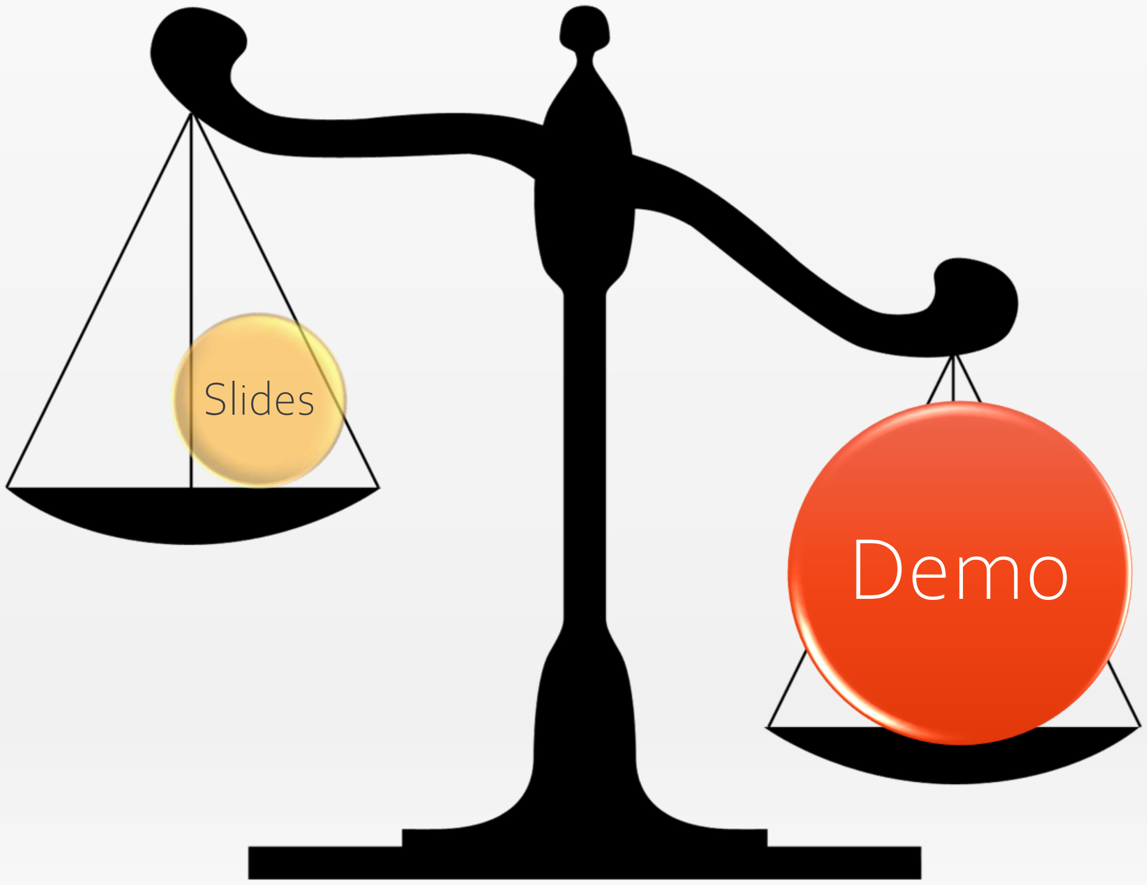
github.com/AndiBellstedt

IT infrastructure guy and PowerShell fellow

Microsoft Infrastructure

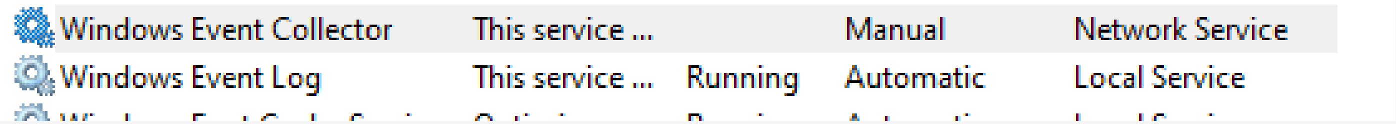
Security

What to expect



Basics about Windows Event Forwarding platform

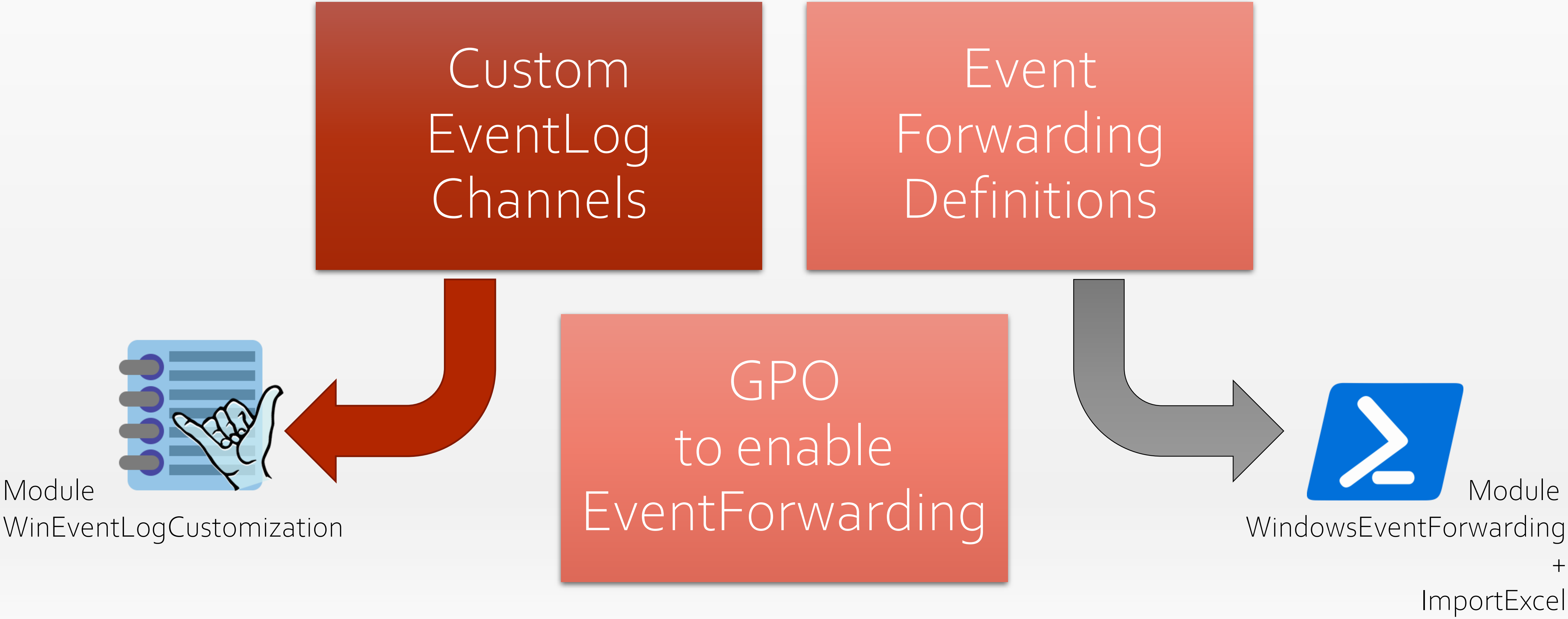
- For free in every Windows available
- Service Windows Event Collector



Windows Event Collector	This service ...		Manual	Network Service
Windows Event Log	This service ...	Running	Automatic	Local Service

- Works for EventLogs in EventLogs
- Two modes for
  - Collector initiated … aka „the dump one“
  - Source initiated … aka „the good one“
- Configuration via GPO recommended

Project Sauron



Custom EventLog Channels

Event Forwarding Definitions

GPO to enable EventForwarding

Module WinEventLogCustomization

Module WindowsEventForwarding + ImportExcel

I WANT LIVE DEMO
DUDE, GO TO CONSOLE
imgflip.com

Question & Answers

Andreas Bellstedt

@AndiBellstedt

github.com/AndiBellstedt

More Information & Links

- Project Sauron
  - https://github.com/russelltomkins/Project-Sauron
  - https://docs.microsoft.com/de-de/archive/blogs/russellt/project-sauron-introduction

- Related Topic
  - PowerShell Module WindowsEventForwarding
    https://github.com/PSSecTools/WindowsEventForwarding
  - PowerShell Module Import-Excel
    https://github.com/dfinke/ImportExcel

- Custom EventLogs
  - WinEventLogCustomization PowerShell Module
    https://github.com/AndiBellstedt/WinEventLogCustomization
  - https://docs.microsoft.com/de-de/archive/blogs/russellt/creating-custom-windows-event-forwarding-logs
  - https://github.com/nsacyber/Event-Forwarding-Guidance

– Thank you –

Andreas Bellstedt

@AndiBellstedt

github.com/AndiBellstedt